日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年 ３月 ５日

出 願 番 号
Application Number: 平成１１年特許願第０５９０４９号

願 人
Applicant (s): 村田機械株式会社
辻井 重男
笠原 正雄

CERTIFIED COPY OF
PRIORITY DOCUMENT

１９９９年 ８月１８日

特 許 庁 長 官
Commissioner,
Patent Office 伴佐山建志

【書類名】　特許願

【整理番号】　20065

【提出日】　平成11年 3月 5日

【あて先】　特許庁長官殿

【国際特許分類】　H04L 9/14

H04L 9/30

G09C 1/00

【発明の名称】　秘密鍵生成方法，暗号化方法及び暗号通信方法

【請求項の数】　3

【発明者】

【住所又は居所】　東京都渋谷区神宮前４－２－１９

【氏名】　辻井　重男

【発明者】

【住所又は居所】　大阪府箕面市粟生外院４丁目１５番３号

【氏名】　笠原　正雄

【発明者】

【住所又は居所】　京都府京都市伏見区竹田向代町１３６番地　村田機械株式会社　本社工場内

【氏名】　村上　恭通

【特許出願人】

【識別番号】　000006297

【氏名又は名称】　村田機械株式会社

【代表者】　村田　純一

【特許出願人】

【住所又は居所】　東京都渋谷区神宮前４－２－１９

【氏名又は名称】　辻井　重男

【特許出願人】

【識別番号】　597008636

【氏名又は名称】　笠原　正雄

【代理人】

【識別番号】　100078868

【弁理士】

【氏名又は名称】　河野　登夫

【電話番号】　06-6944-4141

【手数料の表示】

【予納台帳番号】　001889

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9805283

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　秘密鍵生成方法，暗号化方法及び暗号通信方法

【特許請求の範囲】

【請求項１】　エンティティの特定情報を複数のブロックに分割した分割特定情報を利用して、前記エンティティ固有の秘密鍵を生成する方法において、第１ブロックの分割特定情報に対する秘密鍵を複層構造とし、残りのブロックの分割特定情報に対する秘密鍵を単層構造として前記秘密鍵を生成することを特徴とする秘密鍵生成方法。

【請求項２】　各エンティティの特定情報を複数のブロックに分割した分割特定情報を利用して各エンティティ固有の秘密鍵を生成し、この秘密鍵に含まれている、暗号文の送信先である相手のエンティティの分割特定情報に対応する成分を使用して生成した共通鍵を用いて平文を暗号文に暗号化する暗号化方法において、第１ブロックの分割特定情報に対する秘密鍵を複層構造とし、残りのブロックの分割特定情報に対する秘密鍵を単層構造として各エンティティ固有の秘密鍵を生成することを特徴とする暗号化方法。

【請求項３】　センタから各エンティティへ各エンティティ固有の秘密鍵を送付し、一方のエンティティが前記センタから送付された該エンティティ固有の秘密鍵から求めた共通鍵を用いて平文を暗号文に暗号化して他方のエンティティへ伝送し、該他方のエンティティが伝送された暗号文を、前記センタから送付された該エンティティ固有の秘密鍵から求めた、前記共通鍵と同一の共通鍵を用いて元の平文に復号することにより、エンティティ間で情報の通信を行うこととし、前記センタが複数設けられており、その複数の各センタは、各エンティティの特定情報を複数のブロックに分割した分割特定情報を利用して各エンティティ固有の秘密鍵を生成し、各エンティティは、自身固有の秘密鍵に含まれている、相手のエンティティの分割特定情報に対応する成分を使用して前記共通鍵を生成するようにした暗号通信方法において、第１ブロックの分割特定情報に対する秘密鍵を複層構造とし、残りのブロックの分割特定情報に対する秘密鍵を単層構造として各エンティティ固有の秘密鍵を生成することを特徴とする暗号通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、エンティティ固有の秘密鍵を生成する秘密鍵生成方法、情報の内容が当事者以外にはわからないように情報を暗号化する暗号化方法、及び、暗号文にて通信を行う暗号通信方法に関する。

【０００２】

【従来の技術】

高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤として、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオリジナルとの区別が困難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュータリソースの共有」，「マルチアクセス」，「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事，外交面で用いられてきた暗号技術が注目されている。

【０００３】

暗号とは、情報の意味が当事者以外には理解できないように情報を交換することである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

【０００４】

暗号化鍵と復号鍵とは、等しくても良いし、異なっていても良い。両者の鍵が等しい暗号方式は、共通鍵暗号方式と呼ばれ、米国商務省標準局が採用したＤＥＳ（Data Encryption Standards)はその典型例である。このような共通鍵暗号方

式の従来例は、次のような３種の方法に分類できる。

【０００５】

① 第１の方法

暗号通信を行う可能性がある相手との共通鍵をすべて秘密保管しておく方法。

② 第２の方法

暗号通信の都度、予備通信により鍵を共有し合う方法（Diffie-Hellmanによる鍵共有方式，公開鍵方式による鍵配送方式など）。

③ 第３の方法

各ユーザ（エンティティ）の氏名，住所などの個人を特定する公開された特定情報（ＩＤ（Identity）情報）を利用して、予備通信を行うことなく、送信側のエンティティ，受信側のエンティティが独立に同一の共通鍵を生成する方法（ＫＰＳ（Key Predistribution System），ＩＤ－ＮＩＫＳ（ID-based Non-Interactive Key Sharing Schemes）など）。

【０００６】

【発明が解決しようとする課題】

このような従来の３種の方法には、以下に述べるような問題がある。第１の方法では、すべての共通鍵を保管しておくようにするので、不特定多数のユーザがエンティティとなって暗号通信を行うネットワーク社会には適さない。また、第２の方法は、鍵共有のための予備通信が必要である点が問題である。

【０００７】

第３の方法は、予備通信が不要であり、公開された相手のＩＤ情報とセンタから予め配布されている固有の秘密パラメータとを用いて、任意の相手との共通鍵を生成できるので、便利な方法である。しかしながら、次のような２つの問題点がある。一つは、センタがBig Brother となる（すべてのエンティティの秘密を握っており、Key Escrow System になってしまう）点である。もう一つは、ある数のエンティティが結託するとセンタの秘密を演算できる可能性がある点である。この結託問題については、これを計算量的に回避するための工夫が多数なされているが、完全な解決は困難である。

【０００８】

この結託問題の難しさは、ＩＤ情報に基づく秘密パラメータがセンタ秘密と個人秘密との二重構造になっていることに起因する。第３の方法では、センタの公開パラメータと個人の公開ＩＤ情報とこの２種類の秘密パラメータとにて暗号系が構成され、しかも各エンティティが各自に配布された個人秘密を見せ合ってもセンタ秘密が露呈されないようにする必要がある。よって、その暗号系の構築の実現には解決すべき課題が多い。

【０００９】

そこで、本発明者等は、特定情報（ＩＤ情報）をいくつかに分割し、複数の各センタからその分割した特定情報に基づくすべての秘密鍵をエンティティに配布することにより、数学的構造を最小限に抑えることができて、結託問題の回避を可能にし、その暗号系の構築が容易であるＩＤ－ＮＩＫＳによる秘密鍵生成方法，暗号化方法及び暗号通信方法を提案している（特願平11－16257 号）。

【００１０】

結託問題を解決することを目的として提案されてきたエンティティの特定情報に基づく種々の暗号系が不成功となった理由は、エンティティの結託情報からセンタ秘密を割り出せないようにするための工夫を数学的構造に求め過ぎていたためである。数学的構造が複雑過ぎると、安全性を証明するための方法も困難となる。そこで、特願平11－16257 号の提案方法では、エンティティの特定情報をいくつかに分割し、分割した各特定情報についてすべての秘密鍵をエンティティに配布することにより、数学的構造を最小限に抑えるようにする。この提案方法では、複数のセンタが設けられ、各センタはあるエンティティの分割した１つの特定情報に対応する秘密鍵を生成する。よって、すべてのエンティティの秘密を１つのセンタが握るようなことはなく、各センタがBig Brother にならない。

【００１１】

そして、本発明者等は、この提案方法の改良を研究してきた。特に、特定のエンティティの攻撃に必要なすべてのエンティティを買収し、買収したエンティティの秘密鍵のすべてを用いることにより、その特定のエンティティを攻撃するという乱数置換攻撃に強い改良方法を研究してきた。

【００１２】

本発明は斯かる事情に鑑みてなされたものであり、上記提案方法を改良してより乱数置換攻撃に強くした秘密鍵生成方法，暗号化方法及び暗号通信方法を提供することを目的とする。

【００１３】

【課題を解決するための手段】

請求項１に係る秘密鍵生成方法は、エンティティの特定情報を複数のブロックに分割した分割特定情報を利用して、前記エンティティ固有の秘密鍵を生成する方法において、第１ブロックの分割特定情報に対する秘密鍵を複層構造とし、残りのブロックの分割特定情報に対する秘密鍵を単層構造として前記秘密鍵を生成することを特徴とする。

【００１４】

請求項２に係る暗号化方法は、各エンティティの特定情報を複数のブロックに分割した分割特定情報を利用して各エンティティ固有の秘密鍵を生成し、この秘密鍵に含まれている、暗号文の送信先である相手のエンティティの分割特定情報に対応する成分を使用して生成した共通鍵を用いて平文を暗号文に暗号化する暗号化方法において、第１ブロックの分割特定情報に対する秘密鍵を複層構造とし、残りのブロックの分割特定情報に対する秘密鍵を単層構造として各エンティティ固有の秘密鍵を生成することを特徴とする。

【００１５】

請求項３に係る暗号通信方法は、センタから各エンティティへ各エンティティ固有の秘密鍵を送付し、一方のエンティティが前記センタから送付された該エンティティ固有の秘密鍵から求めた共通鍵を用いて平文を暗号文に暗号化して他方のエンティティへ伝送し、該他方のエンティティが伝送された暗号文を、前記センタから送付された該エンティティ固有の秘密鍵から求めた、前記共通鍵と同一の共通鍵を用いて元の平文に復号することにより、エンティティ間で情報の通信を行うこととし、前記センタが複数設けられており、その複数の各センタは、各エンティティの特定情報を複数のブロックに分割した分割特定情報を利用して各エンティティ固有の秘密鍵を生成し、各エンティティは、自身固有の秘密鍵に含

まれている、相手のエンティティの分割特定情報に対応する成分を使用して前記共通鍵を生成するようにした暗号通信方法において、第１ブロックの分割特定情報に対する秘密鍵を複層構造とし、残りのブロックの分割特定情報に対する秘密鍵を単層構造として各エンティティ固有の秘密鍵を生成することを特徴とする。

【００１６】

本発明では、全ブロックすべての計算を完了して初めて共通鍵が求められるようにしており、特定のエンティティの特定情報の分割ブロックを独立して攻撃できないようになっていて、乱数置換攻撃を回避できる。

【００１７】

【発明の実施の形態】

以下、本発明の実施の形態について具体的に説明する。

図１は、本発明の暗号通信システムの構成を示す模式図である。情報の隠匿を信頼できる複数（Ｋ個）のセンタ１が設定されており、これらのセンタ１としては、例えば社会の公的機関を該当できる。

【００１８】

これらの各センタ１と、この暗号系システムを利用するユーザとしての複数の各エンティティａ，ｂ，…，ｚとは、秘密通信路2_{a1}，…，2_{aK}、2_{b1}，…，2_{bK}、・・・、2_{z1}，…，2_{zK}により接続されており、これらの秘密通信路を介して各センタ１から秘密の鍵情報が各エンティティａ，ｂ，…，ｚへ伝送されるようになっている。また、２人のエンティティの間には通信路３ab，３az，３bz，…が設けられており、この通信路３ab，３az，３bz，…を介して通信情報を暗号化した暗号文が互いのエンティティ間で伝送されるようになっている。

【００１９】

（センタ１での準備処理）

センタ１は以下の公開鍵及び秘密鍵を準備し、公開鍵を公開する。

公開鍵　Ｎ　　Ｎ＝ＰＱ

Ｋ　　ＩＤベクトルの分割ブロック数

M_j　分割したＩＤベクトルのサイズ（ｊ＝１，２，・・・，Ｋ）

Ｌ　　ＩＤベクトルのサイズ（$L=M_1+M_2+\cdots+M_K$）

Ｔ　　指数部分の次数

秘密鍵　Ｐ，Ｑ　　大きな素数

ｇ　　Ｎを法とする最大生成元

H_j　乱数からなる$2^{Mj}\times 2^{Mj}$の対称行列

α_i　エンティティｉの個人秘密乱数

（但し、ｇｃｄ（α_i，λ（Ｎ））＝１，

λ（・）はカーマイケル関数）

β_{ij}　エンティティｉの個人秘密乱数

（但し、$\beta_{i1}+\beta_{i2}+\cdots+\beta_{iK}=\lambda(N)$）

【００２０】

各エンティティの氏名，住所などを示す特定情報であるＩＤベクトルをＬ次元２進ベクトルとし、図２に示すようにそのＩＤベクトルをブロックサイズM_1，M_2，・・・，M_K毎にＫ個のブロックに分割する。例えば、エンティティｉのＩＤベクトル（ベクトルI_i）を式（１）のように分割する。分割特定情報である各ベクトルI_{ij}（ｊ＝１，２，・・・，Ｋ）をＩＤ分割ベクトルと呼ぶ。

【００２１】

【数１】

$$\overrightarrow{I_i}=[\overrightarrow{I_{i1}}\,|\,\overrightarrow{I_{i2}}\,|\cdots|\,\overrightarrow{I_{iK}}] \quad \cdots(1)$$

【００２２】

（エンティティの登録処理）

エンティティｉに登録を依頼された各センタ１は、準備した鍵とエンティティｉのＫ個のＩＤ分割ベクトルについて、それぞれに対応するＫ個の秘密鍵ベクトルs_{ij}（ｊ＝１，２，・・・，Ｋ）を以下の式（2-1），（2-2），・・・，（2-j），・・・，（2-K)に従って計算する。

【００２３】

【数２】

$$\overrightarrow{s_{i1}} = \alpha_i H_1 [\overrightarrow{I_{i1}}] + \beta_{i1} \overrightarrow{1} \quad \cdots (2-1)$$

$$\overrightarrow{s_{i2}} = \alpha_i H_2 [\overrightarrow{I_{i2}}] + \beta_{i2} \overrightarrow{1} \quad \cdots (2-2)$$

$$\vdots$$

$$\overrightarrow{s_{ij}} = \alpha_i H_j [\overrightarrow{I_{ij}}] + \beta_{ij} \overrightarrow{1} \quad \cdots (2-J)$$

$$\vdots$$

$$\overrightarrow{s_{iK}} = \alpha_i H_K [\overrightarrow{I_{iK}}] + \beta_{iK} \overrightarrow{1} \quad \cdots (2-K)$$

【００２４】

但し、ベクトル１は、すべての成分が１であるＫ次元のベクトルを表す。また、H_j［ベクトルI_{ij}］は対称行列H_jからベクトルI_{ij}に対応した行を１行抜き出したものを表し、［・］の操作を参照と定義する。

【００２５】

次に、第１ブロックに関して、（Ｔ＋１）個の秘密鍵ベクトルg_{it}（ｔ＝０，１，２，・・・，Ｔ）を以下の式（3-0），（3-1），（3-2），・・・，（3-t），・・・，（3-T)に従って計算する。

【００２６】

【数３】

$$\overrightarrow{g_{i0}} \equiv g^{\alpha_i^{-T}\overrightarrow{I}} \pmod{N} \quad \cdots(3-0)$$

$$\overrightarrow{g_{i1}} \equiv g^{\alpha_i^{-T}\overrightarrow{s_{i1}}} \pmod{N} \quad \cdots(3-1)$$

$$\overrightarrow{g_{i2}} \equiv g^{\alpha_i^{-T}\langle\overrightarrow{s_{i1}}\rangle^2} \pmod{N} \quad \cdots(3-2)$$

$$\vdots$$

$$\overrightarrow{g_{it}} \equiv g^{\alpha_i^{-T}\langle\overrightarrow{s_{i1}}\rangle^t} \pmod{N} \quad \cdots(3-t)$$

$$\vdots$$

$$\overrightarrow{g_{iT}} \equiv g^{\alpha_i^{-T}\langle\overrightarrow{s_{i1}}\rangle^T} \pmod{N} \quad \cdots(3-T)$$

【００２７】

但し、ｃをスカラー、（４），（５）に示すＡ，Ｂを行列とした場合、$B=c^A$ 及び$B=\langle A\rangle^c$ は、それぞれ（６）及び（７）を表す。

【００２８】

【数４】

$$A=(a_{\mu\nu}) \quad \cdots(4)$$

$$B=(b_{\mu\nu}) \quad \cdots(5)$$

$$b_{\mu\nu}=c^{a_{\mu\nu}} \quad \cdots(6)$$

$$b_{\mu\nu}=a_{\mu\nu}c \quad \cdots(7)$$

【００２９】

そして、１つのセンタ１は、第１ブロックに関する（Ｔ＋１）個の秘密鍵ベクトルg_{it}（ｔ＝０，１，２，・・・，Ｔ）を秘密裏にエンティティｉへ送り、残りの（Ｋ－１）の各センタ１は、第２ブロック以降に関する（Ｋ－１）個の秘密鍵ベクトルs_{ij}（ｊ＝２，３，・・・，Ｋ）を秘密裏にエンティティｉへ送る。

【００３０】

（エンティティ間の共通鍵の生成処理）

エンティティｉは、第１ブロックに関して、自身の（Ｔ＋１）個の秘密鍵ベクトルg_{it}の中から、エンティティｍのＩＤ分割ベクトルであるベクトルI_{m1}に対応する成分のベクトルg_{it}［ベクトルI_{m1}］を選び出す。この選び出したものを(8-0)，(8-1)，・・・，(8-t)，・・・，(8-T)に示す。

【００３１】

【数５】

$$g_{0im} = \overrightarrow{g_{i0}}[\overrightarrow{I_{m1}}] \quad \cdots(8\text{-}0)$$

$$g_{1im} = \overrightarrow{g_{i1}}[\overrightarrow{I_{m1}}] \quad \cdots(8\text{-}1)$$

$$\vdots$$

$$g_{tim} = \overrightarrow{g_{it}}[\overrightarrow{I_{m1}}] \quad \cdots(8\text{-}t)$$

$$\vdots$$

$$g_{Tim} = \overrightarrow{g_{iT}}[\overrightarrow{I_{m1}}] \quad \cdots(8\text{-}T)$$

【００３２】

次に、エンティティｉは、ｊ＝２，３，・・・，Ｋの第２，第３，・・・，第Ｋの各ブロックに関して、自身の秘密鍵ベクトルs_{ij}の中から、エンティティｍのＩＤ分割ベクトルであるベクトルI_{mj}に対応する成分のベクトルs_{ij}［ベクトルI_{mj}］を各ブロック毎に選び出す。この選び出したものを(9-2)，・・・，(9-j)，・・・，(9-K)に示す。

【００３３】

【数６】

$$x_{2im} = \overrightarrow{s_{i2}}[\overrightarrow{I_{m2}}] \quad \cdots(9\text{-}2)$$

$$\vdots$$

$$x_{jim} = \overrightarrow{s_{ij}}[\overrightarrow{I_{mj}}] \quad \cdots(9\text{-}j)$$

$$\vdots$$

$$x_{Kim} = \overrightarrow{s_{iK}}[\overrightarrow{I_{mK}}] \quad \cdots(9\text{-}K)$$

【００３４】

更に、（10）のように整数環上でこれらのすべての和y_{im}を求める。

【００３５】

【数７】

$$y_{im} = \sum_{j=2}^{K} x_{jim} \quad \cdots(10)$$

【００３６】

そして、Ｎを法として以下の（11）のような計算を行うことにより、共通鍵K_{im}を求める。この（11）の計算において、全ブロックの計算を完了することにより、個人秘密乱数α_iはその逆元との乗算にて消去され、Ｋ個の個人秘密乱数β_{ij}はそれらの加算にて消去される。このK_{im}はエンティティｍ側から求めた共通鍵K_{mi}と一致する。

【００３７】

【数８】

$$K_{im} \equiv \prod_{t=0}^{T} g_{t\,im}^{T C_t y_{im}^{(T-t)}}$$

$$\equiv g^{\alpha_i^{-T} \sum_{t=0}^{T} {}_T C_t x_{1im}^{t} y_{im}^{T-t}}$$

$$\equiv g^{\alpha_i^{-T} (x_{1im} + y_{im})^T}$$

$$\equiv g^{\alpha_i^{-T} (x_{1im} + \cdots + x_{Kim})^T}$$

$$\equiv g^{\alpha_i^{-T} (\alpha_i H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}] + \beta_{i1} + \cdots + \alpha_i H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}] + \beta_{iK})^T}$$

$$\equiv g^{\alpha_i^{-T} \{\alpha_i (H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}] + \cdots + H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}]) + \lambda(N)\}^T}$$

$$\equiv g^{\alpha_i^{-T} \{\alpha_i (H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}] + \cdots + H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}])\}^T}$$

$$\equiv g^{(H_i[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}] + \cdots + H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}])^T} \quad (\mathrm{mod}\ N)$$

・・・(11)

【００３８】

なお、上式においてx_{1im}＝ベクトルs_{i1}[ベクトルI_{m1}]と置いたが、これは、エンティティｉ自身にもわからない。また、Ｔは比較的小さな数であるので、指数部分はべき乗を順次繰り返し行うことにより計算することができる。

【００３９】

なお、上記例において、各ブロックのサイズM_jは全ブロックにおいて一定であっても良いし、その一部または全部のブロックで異なっていても良い。しかし、第１ブロックに関して秘密鍵ベクトルg_{it}を求めるので、全ブロックについてそのサイズを一定にした場合、第１ブロックについての秘密が大きくなってしまう。よって、第１ブロックのサイズを他のブロックのサイズよりも小さくするようにした方が良い。特に、M_1＝１とした場合、配布する秘密を最小限にすることができ、最も安全性が高くなる。

【００４０】

ここで、不特定多数のエンティティの結託によって暗号システム全体を攻撃するような結託攻撃に対する本発明の安全性について考察する。エンティティの総数を100 万人とした場合、1000000 ≒2^{20}であるので、M_j ＝１，Ｋ＝20となる。ここで、Ｔ＝32とした場合、共有鍵K_{im}の指数部分の項数は、$_{20}H_{32}=_{51}C_{32}$ ≒4.85×10^{13}となる。この項数は、全エンティティ間の共有鍵の総数 $_{1000000}C_2$ ≒5×10^{12}を超える。よって、項数＞共有鍵の総数の条件を満たし、結託攻撃に対して安全である。

【００４１】

次に、上述した暗号システムにおけるエンティティ間の情報の通信について説明する。図３は、２人のエンティティａ，ｂ間における情報の通信状態を示す模式図である。図３の例は、エンティティａが平文（メッセージ）Ｍを暗号文Ｃに暗号化してそれをエンティティｂへ伝送し、エンティティｂがその暗号文Ｃを元の平文（メッセージ）Ｍに復号する場合を示している。

【００４２】

１番目のセンタ１には、各エンティティａ，ｂ固有の秘密鍵ベクトルs_{a1}，s_{b1}と（Ｔ＋１）個の秘密鍵ベクトルg_{at}，g_{bt}（ｔ＝０，１，２，・・・，Ｔ）とを、前記式 (2-1)と (3-0)，・・・，(3-T)とに従って計算する秘密鍵生成器１ａが備えられている。そして、各エンティティａ，ｂから登録が依頼されると、そのエンティティａ，ｂの秘密鍵ベクトルg_{at}，g_{bt}がエンティティａ，ｂへ送付される。

【００４３】

ｊ（ｊ＝２，３，・・・，Ｋ）番目のセンタ１には、各エンティティａ，ｂ固有の秘密鍵ベクトルs_{aj}，s_{bj}を前記式 (2-2)，・・・，(2-K)に従って計算する秘密鍵生成器１ａが備えられている。そして、各エンティティａ，ｂから登録が依頼されると、そのエンティティａ，ｂの秘密鍵ベクトルs_{aj}，s_{bj}がエンティティａ，ｂへ送付される。

【００４４】

エンティティａ側には、各センタ１から送られるこれらの秘密鍵ベクトルg_{at}

（ｔ＝０，１，２，・・・，Ｔ），s_{aj}（ｊ＝２，３，・・・，Ｋ）をテーブル形式で格納しているメモリ１０と、これらの秘密鍵ベクトルの中からエンティティｂに対応する成分であるベクトルg_{at}［ベクトルI_{bl}］（ｔ＝０，１，２，・・・，Ｔ），ベクトルs_{aj}［ベクトルI_{bj}］（ｊ＝２，３，・・・，Ｋ）を選び出す成分選出器１１と、選び出されたこれらの成分を使用してエンティティａが求めるエンティティｂとの共通鍵K_{ab}を生成する共通鍵生成器１２と、共通鍵K_{ab}を用いて平文（メッセージ）Ｍを暗号文Ｃに暗号化して通信路３０へ出力する暗号化器１３とが備えられている。

【００４５】

また、エンティティｂ側には、各センタ１から送られるこれらの秘密鍵ベクトルg_{bt}（ｔ＝０，１，２，・・・，Ｔ），s_{bj}（ｊ＝２，３，・・・，Ｋ），をテーブル形式で格納しているメモリ２０と、これらの秘密ベクトルの中からエンティティａに対応する成分であるベクトルg_{bt}［ベクトルI_{al}］（ｔ＝０，１，２，・・・，Ｔ），ベクトルs_{bj}［ベクトルI_{aj}］（ｊ＝２，３，・・・，Ｋ）を選び出す成分選出器２１と、選び出されたこれらの成分を使用してエンティティｂが求めるエンティティａとの共通鍵K_{ba}を生成する共通鍵生成器２２と、共通鍵K_{ba}を用いて通信路30から入力した暗号文Ｃを平文Ｍに復号して出力する復号器２３とが備えられている。

【００４６】

エンティティａからエンティティｂへ情報を伝送しようとする場合、まず、各センタ１で求められて、予めメモリ１０に格納されている秘密鍵ベクトルg_{at}（ｔ＝０，１，２，・・・，Ｔ），s_{aj}（ｊ＝２，３，・・・，Ｋ）が成分選出器１１へ読み出される。そして、成分選出器11にて、エンティティｂに対応する成分であるベクトルg_{at}［ベクトルI_{bl}］（ｔ＝０，１，２，・・・，Ｔ），ベクトルs_{aj}［ベクトルI_{bj}］（ｊ＝２，３，・・・，Ｋ）が選び出されて共通鍵生成器１２へ送られる。共通鍵生成器１２にて、これらの成分を使用して（11）に従って共通鍵K_{ab}が求められ、暗号化器１３へ送られる。暗号化器１３において、この共通鍵K_{ab}を用いて平文Ｍが暗号文Ｃに暗号化され、暗号文Ｃが通信路３０を介して伝送される。

【００４７】

通信路３０を伝送された暗号文Ｃはエンティティｂの復号器２３へ入力される。各センタ１で求められて、予めメモリ２０に格納されている秘密鍵ベクトルs_{bj}（ｊ＝２，３，・・・，Ｋ），g_{bt}（ｔ＝０，１，２，・・・，Ｔ）が成分選出器２１へ読み出される。そして、成分選出器２１にて、エンティティａに対応する成分であるベクトルg_{bt}［ベクトルI_{al}］（ｔ＝０，１，２，・・・，Ｔ），ベクトルs_{bj}［ベクトルI_{aj}］（ｊ＝２，３，・・・，Ｋ）が選び出されて共通鍵生成器２２へ送られる。共通鍵生成器２２にて、これらの成分を使用して（11）に従って共通鍵K_{ba}が求められ、復号器２３へ送られる。復号器２３において、この共通鍵K_{ba}を用いて暗号文Ｃが平文Ｍに復号される。

【００４８】

このような例では、複数のセンタが設けられ、各センタはエンティティの分割した１つのＩＤ情報に対応する鍵を生成するようにしたので、すべてのエンティティの秘密を１つのセンタが握るようなことはなく、各センタがBig Brother にならない。また、各エンティティ固有の秘密鍵ベクトルが予めエンティティ側のメモリに格納されているので、共通鍵生成に要する時間が短くて済む。

【００４９】

図４は、本発明の記録媒体の実施の形態の構成を示す図である。ここに例示するプログラムは、各センタからエンティティｉへ送られてくる秘密鍵ベクトルs_{ij}，g_{it}の中からエンティティｍに対応する成分を選び出す処理と、これらの選び出した成分を使用して共通鍵K_{im}を求める処理とを含んでおり、以下に説明する記録媒体に記録されている。なお、コンピュータ４０は、各エンティティ側に設けられている。

【００５０】

図４において、コンピュータ４０とオンライン接続する記録媒体４１は、コンピュータ４０の設置場所から隔たって設置される例えばWWW(World Wide Web)のサーバコンピュータを用いてなり、記録媒体４１には前述の如きプログラム４１ａが記録されている。記録媒体４１から読み出されたプログラム４１ａがコンピュータ４０を制御することにより、各エンティティにおいて通信対象のエンテ

ィティに対する共通鍵を演算する。

【００５１】

コンピュータ４０の内部に設けられた記録媒体４２は、内蔵設置される例えばハードディスクドライブまたはＲＯＭなどを用いてなり、記録媒体４２には前述の如きプログラム４２ａが記録されている。記録媒体４２から読み出されたプログラム４２ａがコンピュータ４０を制御することにより、各エンティティにおいて通信対象のエンティティに対する共通鍵を演算する。

【００５２】

コンピュータ４０に設けられたディスクドライブ４０ａに装填して使用される記録媒体４３は、運搬可能な例えば光磁気ディスク，ＣＤ－ＲＯＭまたはフレキシブルディスクなどを用いてなり、記録媒体４３には前述の如きプログラム４３ａが記録されている。記録媒体４３から読み出されたプログラム４３ａがコンピュータ４０を制御することにより、各エンティティにおいて通信対象のエンティティに対する共通鍵を演算する。

【００５３】

【発明の効果】

以上詳述したように、本発明では、全ブロックすべての計算を完了して初めて乱数項が消去されるようにしているので、分割ブロックを独立して攻撃できないようになっていて、乱数置換攻撃を回避することが可能である。

【００５４】

（付記）

なお、以上の説明に対して更に以下の項を開示する。

（１）　エンティティの特定情報を複数のブロックに分割した分割特定情報を利用して、前記エンティティ固有の秘密鍵を生成する方法において、前記秘密鍵を生成する演算式は以下である秘密鍵生成方法。

【００５５】

【数９】

$$\overrightarrow{s_{i1}} = \alpha_i H_1[\overrightarrow{I_{i1}}] + \beta_{i1}\overrightarrow{1}$$
$$\overrightarrow{s_{i2}} = \alpha_i H_2[\overrightarrow{I_{i2}}] + \beta_{i2}\overrightarrow{1}$$
$$\vdots$$
$$\overrightarrow{s_{ij}} = \alpha_i H_j[\overrightarrow{I_{ij}}] + \beta_{ij}\overrightarrow{1}$$
$$\vdots$$
$$\overrightarrow{s_{iK}} = \alpha_i H_K[\overrightarrow{I_{iK}}] + \beta_{iK}\overrightarrow{1}$$

$$\overrightarrow{g_{i0}} \equiv g^{\alpha_i^{-T}\overrightarrow{1}} \pmod N$$
$$\overrightarrow{g_{i1}} \equiv g^{\alpha_i^{-T}\overrightarrow{s_{i1}}} \pmod N$$
$$\overrightarrow{g_{i2}} \equiv g^{\alpha_i^{-T}\langle\overrightarrow{s_{i1}}\rangle^2} \pmod N$$
$$\vdots$$
$$\overrightarrow{g_{it}} \equiv g^{\alpha_i^{-T}\langle\overrightarrow{s_{i1}}\rangle^t} \pmod N$$
$$\vdots$$
$$\overrightarrow{g_{iT}} \equiv g^{\alpha_i^{-T}\langle\overrightarrow{s_{i1}}\rangle^T} \pmod N$$

【００５６】

但し、

ベクトルs_{ij}：エンティティｉのｊ番目の分割特定情報に対応する秘密鍵（ｊ＝１，２，・・・，Ｋ）

［ベクトルI_{ij}］：エンティティｉのｊ番目の分割特定情報

ベクトル１：成分がすべて１であるＫ次元ベクトル

H_j：乱数からなる$2^{Mj}\times 2^{Mj}$の対称行列

M_j：エンティティｉのｊ番目の分割特定情報のサイズ

Ｋ：エンティティｉの特定情報のブロック分割数

α_i ：エンティティｉの個人秘密乱数

（但し、ｇｃｄ（α_i，λ（Ｎ））＝１，

λ（・）はカーマイケル関数）

Ｎ：Ｎ＝ＰＱ（Ｐ，Ｑは素数）

β_{ij}：エンティティｉの個人秘密乱数

（但し、$\beta_{i1}+\beta_{i2}+\cdots+\beta_{iK}=\lambda(N)$）

ｇ：Ｎを法とする最大生成元

ベクトルg_{it}：エンティティｉの特定情報の第１ブロックに関する秘密鍵（ｔ＝０，１，２，・・・，Ｔ）

Ｔ：指数部分の次数

ｃをスカラーとし、（ｉ），（ii）に示すＡ，Ｂを行列した場合、Ｂ＝c^A及びＢ＝$\langle A\rangle^c$は、それぞれ（iii)及び（iv）を表す

【００５７】

【数１０】

$$A=(a_{\mu\nu}) \quad \cdots(i)$$

$$B=(b_{\mu\nu}) \quad \cdots(ii)$$

$$b_{\mu\nu}=c^{a_{\mu\nu}} \quad \cdots(iii)$$

$$b_{\mu\nu}=a_{\mu\nu}{}^c \quad \cdots(iv)$$

【００５８】

（２）　各エンティティの特定情報を複数のブロックに分割した分割特定情報を利用して各エンティティ固有の秘密鍵を生成し、この秘密鍵に含まれている、暗号文の送信先である相手のエンティティの分割特定情報に対応する成分を使用して生成した共通鍵を用いて平文を暗号文に暗号化する暗号化方法において、各エンティティ固有の秘密鍵を生成する演算式は以下である暗号化方法。

【００５９】

【数１１】

$$\overrightarrow{s_{i1}} = \alpha_i H_1[\overrightarrow{I_{i1}}] + \beta_{i1}\overrightarrow{1}$$

$$\overrightarrow{s_{i2}} = \alpha_i H_2[\overrightarrow{I_{i2}}] + \beta_{i2}\overrightarrow{1}$$

$$\vdots$$

$$\overrightarrow{s_{ij}} = \alpha_i H_j[\overrightarrow{I_{ij}}] + \beta_{ij}\overrightarrow{1}$$

$$\vdots$$

$$\overrightarrow{s_{iK}} = \alpha_i H_K[\overrightarrow{I_{iK}}] + \beta_{iK}\overrightarrow{1}$$

$$\overrightarrow{g_{i0}} \equiv g^{\alpha_i^{-T}\overrightarrow{1}} \pmod N$$

$$\overrightarrow{g_{i1}} \equiv g^{\alpha_i^{-T}\overrightarrow{s_{i1}}} \pmod N$$

$$\overrightarrow{g_{i2}} \equiv g^{\alpha_i^{-T}\langle\overrightarrow{s_{i1}}\rangle^2} \pmod N$$

$$\vdots$$

$$\overrightarrow{g_{it}} \equiv g^{\alpha_i^{-T}\langle\overrightarrow{s_{i1}}\rangle^t} \pmod N$$

$$\vdots$$

$$\overrightarrow{g_{iT}} \equiv g^{\alpha_i^{-T}\langle\overrightarrow{s_{i1}}\rangle^T} \pmod N$$

【００６０】

但し、

ベクトルs_{ij}：エンティティｉのｊ番目の分割特定情報に対応する秘密鍵（ｊ＝１，２，・・・，Ｋ）

［ベクトルI_{ij}］：エンティティｉのｊ番目の分割特定情報

ベクトル１：成分がすべて１であるＫ次元ベクトル

H_j：乱数からなる$2^{Mj}\times 2^{Mj}$の対称行列

M_j：エンティティｉのｊ番目の分割特定情報のサイズ

Ｋ：エンティティｉの特定情報のブロック分割数

α_i ：エンティティｉの個人秘密乱数

（但し、ｇｃｄ（α_i，λ（Ｎ））＝１，

λ（・）はカーマイケル関数）

Ｎ：Ｎ＝ＰＱ（Ｐ，Ｑは素数）

β_{ij}：エンティティｉの個人秘密乱数

（但し、$\beta_{i1}+\beta_{i2}+\cdots+\beta_{iK}=\lambda(N)$）

ｇ：Ｎを法とする最大生成元

ベクトルg_{it}：エンティティｉの特定情報の第１ブロックに関する秘密鍵（ｔ＝０，１，２，・・・，Ｔ）

Ｔ：指数部分の次数

ｃをスカラーとし、（ｉ），（ii）に示すＡ，Ｂを行列した場合、Ｂ＝c^A及びＢ＝$\langle A\rangle^c$は、それぞれ（iii)及び（iv）を表す

【００６１】

【数１２】

$$A=(a_{\mu\nu}) \quad \cdots(i)$$

$$B=(b_{\mu\nu}) \quad \cdots(ii)$$

$$b_{\mu\nu}=c^{a_{\mu\nu}} \quad \cdots(iii)$$

$$b_{\mu\nu}=a_{\mu\nu}{}^{c} \quad \cdots(iv)$$

【００６２】

（３）　第（２）項記載の暗号化方法であって、前記共通鍵を生成する演算式は以下である暗号化方法。

【００６３】

【数１３】

$$
\begin{aligned}
g_{0im} &= \overrightarrow{g_{i0}}[\overrightarrow{I_{m1}}] \\
g_{1im} &= \overrightarrow{g_{i1}}[\overrightarrow{I_{m1}}] \\
&\vdots \\
g_{tim} &= \overrightarrow{g_{it}}[\overrightarrow{I_{m1}}] \\
&\vdots \\
g_{Tim} &= \overrightarrow{g_{iT}}[\overrightarrow{I_{m1}}] \\
x_{2im} &= \overrightarrow{s_{i2}}[\overrightarrow{I_{m2}}] \\
&\vdots \\
x_{jim} &= \overrightarrow{s_{ij}}[\overrightarrow{I_{mj}}] \\
&\vdots \\
x_{Kim} &= \overrightarrow{s_{iK}}[\overrightarrow{I_{mK}}]
\end{aligned}
$$

$$
\begin{aligned}
K_{im} &\equiv \prod_{t=0}^{T} g_{tim}^{{}_{T}C_{t}\, y_{im}^{(T-t)}} \\
&\equiv g^{\alpha_i^{-T} \sum_{t=0}^{T} {}_{T}C\, x_{1im}^{t}\, y_{im}^{T-t}} \\
&\equiv g^{\alpha_i^{-T} (x_{1im}+y_{im})^{T}} \\
&\equiv g^{\alpha_i^{-T} (x_{1im}+\cdots+x_{Kim})^{T}} \\
&\equiv g^{\alpha_i^{-T} (\alpha_i H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}]+\beta_{i1}+\cdots+\alpha_i H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}]+\beta_{iK})^{T}} \\
&\equiv g^{\alpha_i^{-T} \{\alpha_i (H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}]+\cdots+H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}])+\lambda(N)\}^{T}} \\
&\equiv g^{\alpha_i^{-T} \{\alpha_i (H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}]+\cdots+H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}])\}^{T}} \\
&\equiv g^{(H_i[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}]+\cdots+H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}])^{T}} \quad (\mathrm{mod}\ N)
\end{aligned}
$$

【００６４】

但し、

g_{tim} （＝ベクトルg_{it}［ベクトルI_{ml}］）

：エンティティｉの特定情報の第１ブロックについて自身のベクトルg_{it}から選び出した、エンティティｍのベクトルI_{ml}に対応する成分（ｔ＝０，１，２，・・・，Ｔ）

x_{1im} ＝ベクトルs_{i1}［ベクトルI_{ml}］

x_{jim} （＝ベクトルs_{ij}［ベクトルI_{mj}］）

：エンティティｉの特定情報の第ｊブロックについて自身のベクトルs_{ij}から選び出した、エンティティｍのベクトルI_{mj}に対応する成分（ｊ＝２，３，・・・，Ｋ）

K_{im}：一方のエンティティｉが他方のエンティティｍに対して生成する共通鍵

y_{im}：（Ｋ－１）個のx_{jim}の和（ｊ＝２，３，・・・，Ｋ）

即ち、$y_{im}=x_{2im}+x_{3im}+\cdots+x_{Kim}$

【００６５】

（４）　センタから各エンティティへ各エンティティ固有の秘密鍵を送付し、一方のエンティティが前記センタから送付された該エンティティ固有の秘密鍵から求めた共通鍵を用いて平文を暗号文に暗号化して他方のエンティティへ伝送し、該他方のエンティティが伝送された暗号文を、前記センタから送付された該エンティティ固有の秘密鍵から求めた、前記共通鍵と同一の共通鍵を用いて元の平文に復号することにより、エンティティ間で情報の通信を行うこととし、前記センタが複数設けられており、その複数の各センタは、各エンティティの特定情報を複数のブロックに分割した分割特定情報を利用して各エンティティ固有の秘密鍵を生成し、各エンティティは、自身固有の秘密鍵に含まれている、相手のエンティティの分割特定情報に対応する成分を使用して前記共通鍵を生成するようにした暗号通信方法において、前記センタにおける秘密鍵を生成する演算式は以下である暗号通信方法。

【００６６】

【数１４】

$$\overrightarrow{s_{i1}} = \alpha_i H_1[\overrightarrow{I_{i1}}] + \beta_{i1}\overrightarrow{1}$$

$$\overrightarrow{s_{i2}} = \alpha_i H_2[\overrightarrow{I_{i2}}] + \beta_{i2}\overrightarrow{1}$$

$$\vdots$$

$$\overrightarrow{s_{ij}} = \alpha_i H_j[\overrightarrow{I_{ij}}] + \beta_{ij}\overrightarrow{1}$$

$$\vdots$$

$$\overrightarrow{s_{iK}} = \alpha_i H_K[\overrightarrow{I_{iK}}] + \beta_{iK}\overrightarrow{1}$$

$$\overrightarrow{g_{i0}} \equiv g^{\alpha_i^{-T}\overrightarrow{1}} \pmod N$$

$$\overrightarrow{g_{i1}} \equiv g^{\alpha_i^{-T}\overrightarrow{s_{i1}}} \pmod N$$

$$\overrightarrow{g_{i2}} \equiv g^{\alpha_i^{-T}\langle\overrightarrow{s_{i1}}\rangle^2} \pmod N$$

$$\vdots$$

$$\overrightarrow{g_{it}} \equiv g^{\alpha_i^{-T}\langle\overrightarrow{s_{i1}}\rangle^t} \pmod N$$

$$\vdots$$

$$\overrightarrow{g_{iT}} \equiv g^{\alpha_i^{-T}\langle\overrightarrow{s_{i1}}\rangle^T} \pmod N$$

【００６７】

但し、

ベクトルs_{ij}：エンティティｉのｊ番目の分割特定情報に対応する秘密鍵（ｊ＝１，２，・・・，Ｋ）

［ベクトルI_{ij}］：エンティティｉのｊ番目の分割特定情報

ベクトル１：成分がすべて１であるＫ次元ベクトル

H_j：乱数からなる$2^{Mj}\times 2^{Mj}$の対称行列

M_j：エンティティｉのｊ番目の分割特定情報のサイズ

Ｋ：エンティティｉの特定情報のブロック分割数

α_i：エンティティｉの個人秘密乱数

（但し、ｇｃｄ（α_i，λ（Ｎ））＝１，

λ（・）はカーマイケル関数）

Ｎ：Ｎ＝ＰＱ（Ｐ，Ｑは素数）

β_{ij}：エンティティｉの個人秘密乱数

（但し、$\beta_{i1}+\beta_{i2}+\cdots+\beta_{iK}=\lambda(N)$）

ｇ：Ｎを法とする最大生成元

ベクトルg_{it}：エンティティｉの特定情報の第１ブロックに関する秘密鍵（ｔ＝０，１，２，・・・，Ｔ）

Ｔ：指数部分の次数

ｃをスカラーとし、（ｉ），（ii）に示すＡ，Ｂを行列した場合、Ｂ＝c^A及びＢ＝$\langle A\rangle^c$は、それぞれ（iii)及び（iv）を表す

【００６８】

【数１５】

$$A=(a_{\mu\nu}) \quad \cdots(i)$$

$$B=(b_{\mu\nu}) \quad \cdots(ii)$$

$$b_{\mu\nu}=c^{a_{\mu\nu}} \quad \cdots(iii)$$

$$b_{\mu\nu}=a_{\mu\nu}{}^{c} \quad \cdots(iv)$$

【００６９】

（５）　第（４）項記載の暗号通信方法であって、前記共通鍵を生成する演算式は以下である暗号通信方法。

【００７０】

【数１６】

$$g_{0im} = \overrightarrow{g_{i0}}[\overrightarrow{I_{m1}}]$$
$$g_{1im} = \overrightarrow{g_{i1}}[\overrightarrow{I_{m1}}]$$
$$\vdots$$
$$g_{tim} = \overrightarrow{g_{it}}[\overrightarrow{I_{m1}}]$$
$$\vdots$$
$$g_{Tim} = \overrightarrow{g_{iT}}[\overrightarrow{I_{m1}}]$$

$$x_{2im} = \overrightarrow{s_{i2}}[\overrightarrow{I_{m2}}]$$
$$\vdots$$
$$x_{jim} = \overrightarrow{s_{ij}}[\overrightarrow{I_{mj}}]$$
$$\vdots$$
$$x_{Kim} = \overrightarrow{s_{iK}}[\overrightarrow{I_{mK}}]$$

$$K_{im} \equiv \prod_{t=0}^{T} g_{tim}^{T C_t y_{im}^{(T-t)}}$$
$$\equiv g^{\alpha_i^{-T} \sum_{t=0}^{T} {}_T C_t x_{1im}^{t} y_{im}^{T-t}}$$
$$\equiv g^{\alpha_i^{-T} (x_{1im}+y_{im})^T}$$
$$\equiv g^{\alpha_i^{-T} (x_{1im}+\cdots+x_{Kim})^T}$$
$$\equiv g^{\alpha_i^{-T}(\alpha_i H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}]+\beta_{i1}+\cdots+\alpha_i H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}]+\beta_{iK})^T}$$
$$\equiv g^{\alpha_i^{-T}\{\alpha_i(H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}]+\cdots+H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}])+\lambda(N)\}^T}$$
$$\equiv g^{\alpha_i^{-T}\{\alpha_i(H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}]+\cdots+H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}])\}^T}$$
$$\equiv g^{(H_i[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}]+\cdots+H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}])^T} \quad (\mathrm{mod}\ N)$$

【００７１】

但し、

g_{tim} （＝ベクトルg_{it}［ベクトルI_{ml}］）

：エンティティｉの特定情報の第１ブロックについて自身のベクトルg_{it}から選び出した、エンティティｍのベクトルI_{ml}に対応する成分（ｔ＝０，１，２，・・・，Ｔ）

x_{1im} ＝ベクトルs_{i1}［ベクトルI_{ml}］

x_{jim} （＝ベクトルs_{ij}［ベクトルI_{mj}］）

：エンティティｉの特定情報の第ｊブロックについて自身のベクトルs_{ij}から選び出した、エンティティｍのベクトルI_{mj}に対応する成分（ｊ＝２，３，・・・，Ｋ）

K_{im}：一方のエンティティｉが他方のエンティティｍに対して生成する共通鍵

y_{im}：（Ｋ－１）個のx_{jim}の和（ｊ＝２，３，・・・，Ｋ）

即ち、$y_{im}=x_{2im}+x_{3im}+\cdots+x_{Kim}$

【００７２】

（６）　暗号通信システムのエンティティに設けられており、平文から暗号文への暗号化処理及び暗号文から平文への復号処理に用いる共通鍵を生成する共通鍵生成装置において、前記エンティティの特定情報を複数のブロックに分割した分割特定情報毎に以下の演算式に従って作成された前記エンティティ固有の秘密鍵を格納する格納手段と、格納されている秘密鍵の中から、通信相手のエンティティの分割特定情報に対応する成分を選び出す選出手段と、選び出した成分を使用して以下の演算式に従って前記共通鍵を生成する手段とを備える共通鍵生成装置。

【００７３】

【数１７】

$$\overrightarrow{s_{i1}} = \alpha_i H_1[\overrightarrow{I_{i1}}] + \beta_{i1}\overrightarrow{1}$$

$$\overrightarrow{s_{i2}} = \alpha_i H_2[\overrightarrow{I_{i2}}] + \beta_{i2}\overrightarrow{1}$$

$$\vdots$$

$$\overrightarrow{s_{ij}} = \alpha_i H_j[\overrightarrow{I_{ij}}] + \beta_{ij}\overrightarrow{1}$$

$$\vdots$$

$$\overrightarrow{s_{iK}} = \alpha_i H_K[\overrightarrow{I_{iK}}] + \beta_{iK}\overrightarrow{1}$$

$$\overrightarrow{g_{i0}} \equiv g^{\alpha_i^{-T}\overrightarrow{1}} \pmod N$$

$$\overrightarrow{g_{i1}} \equiv g^{\alpha_i^{-T}\overrightarrow{s_{i1}}} \pmod N$$

$$\overrightarrow{g_{i2}} \equiv g^{\alpha_i^{-T}\langle\overrightarrow{s_{i1}}\rangle^2} \pmod N$$

$$\vdots$$

$$\overrightarrow{g_{it}} \equiv g^{\alpha_i^{-T}\langle\overrightarrow{s_{i1}}\rangle^t} \pmod N$$

$$\vdots$$

$$\overrightarrow{g_{iT}} \equiv g^{\alpha_i^{-T}\langle\overrightarrow{s_{i1}}\rangle^T} \pmod N$$

【００７４】

但し、

ベクトルs_{ij}：エンティティｉのｊ番目の分割特定情報に対応する秘密鍵（ｊ＝１，２，・・・，Ｋ）

［ベクトルI_{ij}］：エンティティｉのｊ番目の分割特定情報

ベクトル１：成分がすべて１であるＫ次元ベクトル

H_j：乱数からなる$2^{Mj}\times 2^{Mj}$の対称行列

M_j：エンティティｉのｊ番目の分割特定情報のサイズ

Ｋ：エンティティｉの特定情報のブロック分割数

α_i ：エンティティｉの個人秘密乱数

（但し、ｇｃｄ（α_i，λ（Ｎ））＝１，

λ（・）はカーマイケル関数）

Ｎ：Ｎ＝ＰＱ（Ｐ，Ｑは素数）

β_{ij}：エンティティｉの個人秘密乱数

（但し、$\beta_{i1}+\beta_{i2}+\cdots+\beta_{iK}=\lambda(N)$）

ｇ：Ｎを法とする最大生成元

ベクトルg_{it}：エンティティｉの特定情報の第１ブロックに関する秘密鍵（ｔ＝０，１，２，・・・，Ｔ）

Ｔ：指数部分の次数

ｃをスカラーとし、（ｉ），（ii）に示すＡ，Ｂを行列した場合、Ｂ＝c^A及びＢ＝$\langle A\rangle^c$は、それぞれ（iii)及び（iv）を表す

【００７５】

【数１８】

$$A=(a_{\mu\nu}) \quad \cdots(i)$$

$$B=(b_{\mu\nu}) \quad \cdots(ii)$$

$$b_{\mu\nu}=c^{a_{\mu\nu}} \quad \cdots(iii)$$

$$b_{\mu\nu}=a_{\mu\nu}{}^{c} \quad \cdots(iv)$$

【００７６】

【数１９】

$$
\begin{aligned}
g_{0im} &= \overrightarrow{g_{i0}}[\overrightarrow{I_{m1}}] \\
g_{1im} &= \overrightarrow{g_{i1}}[\overrightarrow{I_{m1}}] \\
&\vdots \\
g_{tim} &= \overrightarrow{g_{it}}[\overrightarrow{I_{m1}}] \\
&\vdots \\
g_{Tim} &= \overrightarrow{g_{iT}}[\overrightarrow{I_{m1}}] \\
x_{2im} &= \overrightarrow{s_{i2}}[\overrightarrow{I_{m2}}] \\
&\vdots \\
x_{jim} &= \overrightarrow{s_{ij}}[\overrightarrow{I_{mj}}] \\
&\vdots \\
x_{Kim} &= \overrightarrow{s_{iK}}[\overrightarrow{I_{mK}}]
\end{aligned}
$$

$$
\begin{aligned}
K_{im} &\equiv \prod_{t=0}^{T} g_{tim}^{T C_t y_{im}^{(T-t)}} \\
&\equiv g^{\alpha_i^{-T} \sum_{t=0}^{T} {}_T C_t x_{1im}^{t} y_{im}^{T-t}} \\
&\equiv g^{\alpha_i^{-T} (x_{1im}+y_{im})^T} \\
&\equiv g^{\alpha_i^{-T} (x_{1im}+\cdots+x_{Kim})^T} \\
&\equiv g^{\alpha_i^{-T}(\alpha_i H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}]+\beta_{i1}+\cdots+\alpha_i H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}]+\beta_{iK})^T} \\
&\equiv g^{\alpha_i^{-T}\{\alpha_i(H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}]+\cdots+H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}])+\lambda(N)\}^T} \\
&\equiv g^{\alpha_i^{-T}\{\alpha_i(H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}]+\cdots+H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}])\}^T} \\
&\equiv g^{(H_i[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}]+\cdots+H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}])^T} \quad (\mathrm{mod}\ N)
\end{aligned}
$$

【００７７】

但し、

g_{tim} （＝ベクトルg_{it}［ベクトルI_{ml}］）

：エンティティｉの特定情報の第ｌブロックについて自身のベクトルg_{it}から選び出した、エンティティｍのベクトルI_{ml}に対応する成分（ｔ＝０，１，２，・・・，Ｔ）

x_{lim} ＝ベクトルs_{il}［ベクトルI_{ml}］

x_{jim} （＝ベクトルs_{ij}［ベクトルI_{mj}］）

：エンティティｉの特定情報の第ｊブロックについて自身のベクトルs_{ij}から選び出した、エンティティｍのベクトルI_{mj}に対応する成分（ｊ＝２，３，・・・，Ｋ）

K_{im}：一方のエンティティｉが他方のエンティティｍに対して生成する共通鍵

y_{im}：（Ｋ－１）個のx_{jim}の和（ｊ＝２，３，・・・，Ｋ）

即ち、$y_{im}=x_{2im}+x_{3im}+\cdots+x_{Kim}$

【００７８】

（７）　送信すべき情報である平文を暗号文に暗号化する暗号化処理、及び、送信された暗号文を元の平文に復号する復号処理を、複数のエンティティ間で相互に行う暗号通信システムにおいて、各エンティティの特定情報を複数のブロックに分割した分割特定情報を利用して以下の演算式に従い各エンティティ固有の秘密鍵を生成して各エンティティへ送付する複数のセンタと、該センタから送付された自身の秘密鍵に含まれている、通信対象のエンティティの分割特定情報に対応する成分を使用して以下の演算式に従い、前記暗号化処理及び復号処理に用いる共通鍵を生成する複数のエンティティとを有する暗号通信システム。

【００７９】

【数２０】

$$\overrightarrow{s_{i1}} = \alpha_i H_1[\overrightarrow{I_{i1}}] + \beta_{i1}\overrightarrow{1}$$

$$\overrightarrow{s_{i2}} = \alpha_i H_2[\overrightarrow{I_{i2}}] + \beta_{i2}\overrightarrow{1}$$

$$\vdots$$

$$\overrightarrow{s_{ij}} = \alpha_i H_j[\overrightarrow{I_{ij}}] + \beta_{ij}\overrightarrow{1}$$

$$\vdots$$

$$\overrightarrow{s_{iK}} = \alpha_i H_K[\overrightarrow{I_{iK}}] + \beta_{iK}\overrightarrow{1}$$

$$\overrightarrow{g_{i0}} \equiv g^{\alpha_i^{-T}\overrightarrow{1}} \pmod N$$

$$\overrightarrow{g_{i1}} \equiv g^{\alpha_i^{-T}\overrightarrow{s_{i1}}} \pmod N$$

$$\overrightarrow{g_{i2}} \equiv g^{\alpha_i^{-T}\langle\overrightarrow{s_{i1}}\rangle^2} \pmod N$$

$$\vdots$$

$$\overrightarrow{g_{it}} \equiv g^{\alpha_i^{-T}\langle\overrightarrow{s_{i1}}\rangle^t} \pmod N$$

$$\vdots$$

$$\overrightarrow{g_{iT}} \equiv g^{\alpha_i^{-T}\langle\overrightarrow{s_{i1}}\rangle^T} \pmod N$$

【００８０】

但し、

ベクトルs_{ij}：エンティティｉのｊ番目の分割特定情報に対応する秘密鍵（ｊ＝１，２，・・・，Ｋ）

［ベクトルI_{ij}］：エンティティｉのｊ番目の分割特定情報

ベクトル１：成分がすべて１であるＫ次元ベクトル

H_j：乱数からなる$2^{Mj}\times 2^{Mj}$の対称行列

M_j：エンティティｉのｊ番目の分割特定情報のサイズ

Ｋ：エンティティｉの特定情報のブロック分割数

α_i ：エンティティｉの個人秘密乱数

（但し、ｇｃｄ（α_i，λ（Ｎ））＝１，

λ（・）はカーマイケル関数）

Ｎ：Ｎ＝ＰＱ（Ｐ，Ｑは素数）

β_{ij}：エンティティｉの個人秘密乱数

（但し、$\beta_{i1}+\beta_{i2}+\cdots+\beta_{iK}=\lambda(N)$）

ｇ：Ｎを法とする最大生成元

ベクトルg_{it}：エンティティｉの特定情報の第１ブロックに関する秘密鍵（ｔ＝０，１，２，・・・，Ｔ）

Ｔ：指数部分の次数

ｃをスカラーとし、（ｉ），（ii）に示すＡ，Ｂを行列した場合、Ｂ＝c^{A}及びＢ＝$\langle A\rangle^{c}$は、それぞれ（iii)及び（iv）を表す

【００８１】

【数２１】

$$A=(a_{\mu\nu}) \quad \cdots(i)$$

$$B=(b_{\mu\nu}) \quad \cdots(ii)$$

$$b_{\mu\nu}=c^{a_{\mu\nu}} \quad \cdots(iii)$$

$$b_{\mu\nu}=a_{\mu\nu}{}^{c} \quad \cdots(iv)$$

【００８２】

【数２２】

$$g_{0im}=\overrightarrow{g_{i0}}[\overrightarrow{I_{m1}}]$$
$$g_{1im}=\overrightarrow{g_{i1}}[\overrightarrow{I_{m1}}]$$
$$\vdots$$
$$g_{tim}=\overrightarrow{g_{it}}[\overrightarrow{I_{m1}}]$$
$$\vdots$$
$$g_{Tim}=\overrightarrow{g_{iT}}[\overrightarrow{I_{m1}}]$$

$$x_{2im}=\overrightarrow{s_{i2}}[\overrightarrow{I_{m2}}]$$
$$\vdots$$
$$x_{jim}=\overrightarrow{s_{ij}}[\overrightarrow{I_{mj}}]$$
$$\vdots$$
$$x_{Kim}=\overrightarrow{s_{iK}}[\overrightarrow{I_{mK}}]$$

$$K_{im}\equiv\prod_{t=0}^{T} g_{tim}^{T C_t y_{im}^{(T-t)}}$$
$$\equiv g^{\alpha_i^{-T}\sum_{t=0}^{T}{}_T C_t x_{1im}^{t} y_{im}^{T-t}}$$
$$\equiv g^{\alpha_i^{-T}(x_{1im}+y_{im})^T}$$
$$\equiv g^{\alpha_i^{-T}(x_{1im}+\cdots+x_{Kim})^T}$$
$$\equiv g^{\alpha_i^{-T}(\alpha_i H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}]+\beta_{i1}+\cdots+\alpha_i H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}]+\beta_{iK})^T}$$
$$\equiv g^{\alpha_i^{-T}\{\alpha_i(H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}]+\cdots+H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}])+\lambda(N)\}^T}$$
$$\equiv g^{\alpha_i^{-T}\{\alpha_i(H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}]+\cdots+H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}])\}^T}$$
$$\equiv g^{(H_i[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}]+\cdots+H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}])^T}\ (\mathrm{mod}\ N)$$

【００８３】

但し、

g_{tim} （＝ベクトルg_{it}［ベクトルI_{ml}］）

：エンティティｉの特定情報の第１ブロックについて自身のベクトルg_{it}から選び出した、エンティティｍのベクトルI_{ml}に対応する成分（ｔ＝０，１，２，・・・，Ｔ）

x_{lim} ＝ベクトルs_{il}［ベクトルI_{ml}］

x_{jim} （＝ベクトルs_{ij}［ベクトルI_{mj}］）

：エンティティｉの特定情報の第ｊブロックについて自身のベクトルs_{ij}から選び出した、エンティティｍのベクトルI_{mj}に対応する成分（ｊ＝２，３，・・・，Ｋ）

K_{im}：一方のエンティティｉが他方のエンティティｍに対して生成する共通鍵

y_{im}：（Ｋ－１）個のx_{jim}の和（ｊ＝２，３，・・・，Ｋ）

即ち、$y_{im}=x_{2im}+x_{3im}+\cdots+x_{Kim}$

【００８４】

（８）　暗号通信システムにおける平文から暗号文への暗号化処理及び暗号文から平文への復号処理に用いる共通鍵をエンティティ側で生成するためのプログラムを記録してあるコンピュータでの読み取り可能な記録媒体において、前記エンティティの特定情報を複数のブロックに分割した分割特定情報毎に以下の演算式に従って作成された前記エンティティ固有の秘密鍵の中から、通信相手のエンティティの分割特定情報に対応する成分を選び出すことを前記コンピュータにさせるプログラムコード手段と、選び出した成分を使用して以下の演算式に従って前記共通鍵を生成することを前記コンピュータにさせるプログラムコード手段とを有する記録媒体。

【００８５】

【数２３】

$$\overrightarrow{s_{i1}} = \alpha_i H_1[\overrightarrow{I_{i1}}] + \beta_{i1}\overrightarrow{1}$$

$$\overrightarrow{s_{i2}} = \alpha_i H_2[\overrightarrow{I_{i2}}] + \beta_{i2}\overrightarrow{1}$$

$$\vdots$$

$$\overrightarrow{s_{ij}} = \alpha_i H_j[\overrightarrow{I_{ij}}] + \beta_{ij}\overrightarrow{1}$$

$$\vdots$$

$$\overrightarrow{s_{iK}} = \alpha_i H_K[\overrightarrow{I_{iK}}] + \beta_{iK}\overrightarrow{1}$$

$$\overrightarrow{g_{i0}} \equiv g^{\alpha_i^{-T}\overrightarrow{1}} \pmod N$$

$$\overrightarrow{g_{i1}} \equiv g^{\alpha_i^{-T}\overrightarrow{s_{i1}}} \pmod N$$

$$\overrightarrow{g_{i2}} \equiv g^{\alpha_i^{-T}\langle\overrightarrow{s_{i1}}\rangle^2} \pmod N$$

$$\vdots$$

$$\overrightarrow{g_{it}} \equiv g^{\alpha_i^{-T}\langle\overrightarrow{s_{i1}}\rangle^t} \pmod N$$

$$\vdots$$

$$\overrightarrow{g_{iT}} \equiv g^{\alpha_i^{-T}\langle\overrightarrow{s_{i1}}\rangle^T} \pmod N$$

【００８６】

但し、

ベクトルs_{ij}：エンティティｉのｊ番目の分割特定情報に対応する秘密鍵（ｊ＝１，２，・・・，Ｋ）

［ベクトルI_{ij}］：エンティティｉのｊ番目の分割特定情報

ベクトル１：成分がすべて１であるＫ次元ベクトル

H_j：乱数からなる$2^{Mj}\times 2^{Mj}$の対称行列

M_j：エンティティｉのｊ番目の分割特定情報のサイズ

Ｋ：エンティティｉの特定情報のブロック分割数

α_i ：エンティティｉの個人秘密乱数

（但し、ｇｃｄ（α_i，λ（Ｎ））＝１，

λ（・）はカーマイケル関数）

Ｎ：Ｎ＝ＰＱ（Ｐ，Ｑは素数）

β_{ij}：エンティティｉの個人秘密乱数

（但し、$\beta_{i1}+\beta_{i2}+\cdots+\beta_{iK}=\lambda(N)$）

ｇ：Ｎを法とする最大生成元

ベクトルg_{it}：エンティティｉの特定情報の第１ブロックに関する秘密鍵（ｔ＝０，１，２，・・・，Ｔ）

Ｔ：指数部分の次数

ｃをスカラーとし、（ｉ），（ii）に示すＡ，Ｂを行列した場合、Ｂ＝c^A及びＢ＝$\langle A\rangle^c$は、それぞれ（iii)及び（iv）を表す

【００８７】

【数２４】

$$A=(a_{\mu\nu}) \quad \cdots(i)$$

$$B=(b_{\mu\nu}) \quad \cdots(ii)$$

$$b_{\mu\nu}=c^{a_{\mu\nu}} \quad \cdots(iii)$$

$$b_{\mu\nu}=a_{\mu\nu}{}^{c} \quad \cdots(iv)$$

【００８８】

【数２５】

$$
\begin{aligned}
g_{0im} &= \overrightarrow{g_{i0}}[\overrightarrow{I_{m1}}] \\
g_{1im} &= \overrightarrow{g_{i1}}[\overrightarrow{I_{m1}}] \\
&\vdots \\
g_{tim} &= \overrightarrow{g_{it}}[\overrightarrow{I_{m1}}] \\
&\vdots \\
g_{Tim} &= \overrightarrow{g_{iT}}[\overrightarrow{I_{m1}}] \\
\\
x_{2im} &= \overrightarrow{s_{i2}}[\overrightarrow{I_{m2}}] \\
&\vdots \\
x_{jim} &= \overrightarrow{s_{ij}}[\overrightarrow{I_{mj}}] \\
&\vdots \\
x_{Kim} &= \overrightarrow{s_{iK}}[\overrightarrow{I_{mK}}]
\end{aligned}
$$

$$
\begin{aligned}
K_{im} &\equiv \prod_{t=0}^{T} g_{tim}^{T C_t y_{im}^{(T-t)}} \\
&\equiv g^{\alpha_i^{-T} \sum_{t=0}^{T} {}_T C_t x_{1im}^{t} y_{im}^{T-t}} \\
&\equiv g^{\alpha_i^{-T} (x_{1im}+y_{im})^T} \\
&\equiv g^{\alpha_i^{-T} (x_{1im}+\cdots+x_{Kim})^T} \\
&\equiv g^{\alpha_i^{-T}(\alpha_i H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}]+\beta_{i1}+\cdots+\alpha_i H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}]+\beta_{iK})^T} \\
&\equiv g^{\alpha_i^{-T}\{\alpha_i(H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}]+\cdots+H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}])+\lambda(N)\}^T} \\
&\equiv g^{\alpha_i^{-T}\{\alpha_i(H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}]+\cdots+H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}])\}^T} \\
&\equiv g^{(H_i[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}]+\cdots+H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}])^T} \quad (\mathrm{mod}\ N)
\end{aligned}
$$

【００８９】

但し、

g_{tim} （＝ベクトルg_{it}［ベクトルI_{ml}］）

：エンティティｉの特定情報の第１ブロックについて自身のベクトルg_{it}から選び出した、エンティティｍのベクトルI_{ml}に対応する成分（ｔ＝０，１，２，・・・，Ｔ）

x_{1im} ＝ベクトルs_{i1}［ベクトルI_{ml}］

x_{jim} （＝ベクトルs_{ij}［ベクトルI_{mj}］）

：エンティティｉの特定情報の第ｊブロックについて自身のベクトルs_{ij}から選び出した、エンティティｍのベクトルI_{mj}に対応する成分（ｊ＝２，３，・・・，Ｋ）

K_{im}：一方のエンティティｉが他方のエンティティｍに対して生成する共通鍵

y_{im}：（Ｋ－１）個のx_{jim}の和（ｊ＝２，３，・・・，Ｋ）

即ち、$y_{im}=x_{2im}+x_{3im}+\cdots+x_{Kim}$

【図面の簡単な説明】

【図１】

本発明の暗号通信システムの構成を示す模式図である。

【図２】

エンティティのＩＤベクトルの分割例を示す模式図である。

【図３】

２人のエンティティ間における情報の通信状態を示す模式図である。

【図４】

記録媒体の実施の形態の構成を示す図である。

【符号の説明】

１　センタ

１ａ　秘密鍵生成器

１０，２０　メモリ

１１，２１　成分選出器

１２，２２　共通鍵生成器

１３　暗号化器

２３　復号器

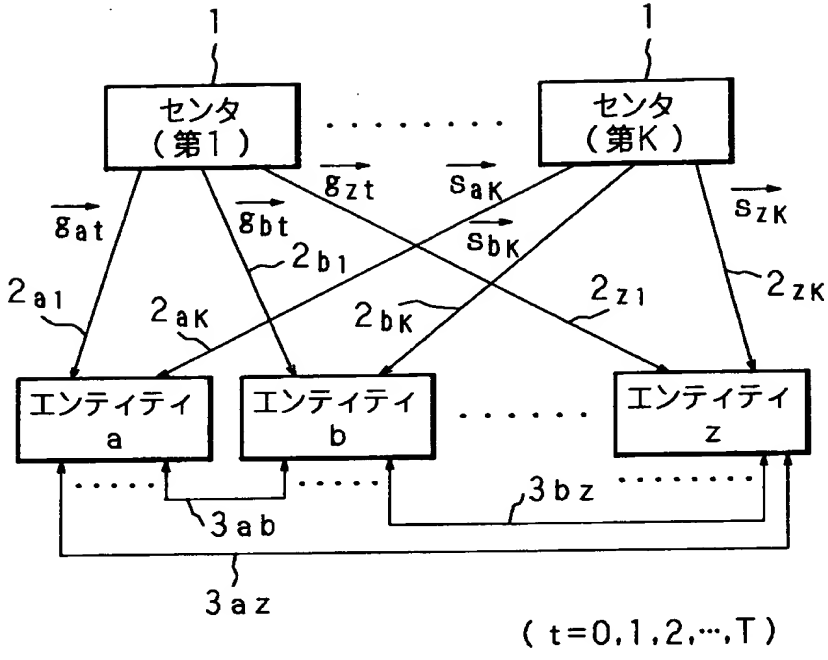
３０　通信路

４０　コンピュータ

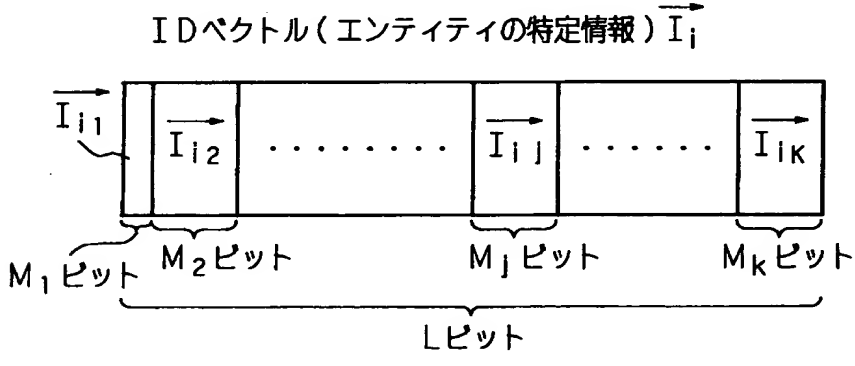
４１，４２，４３　記録媒体

【書類名】　図面

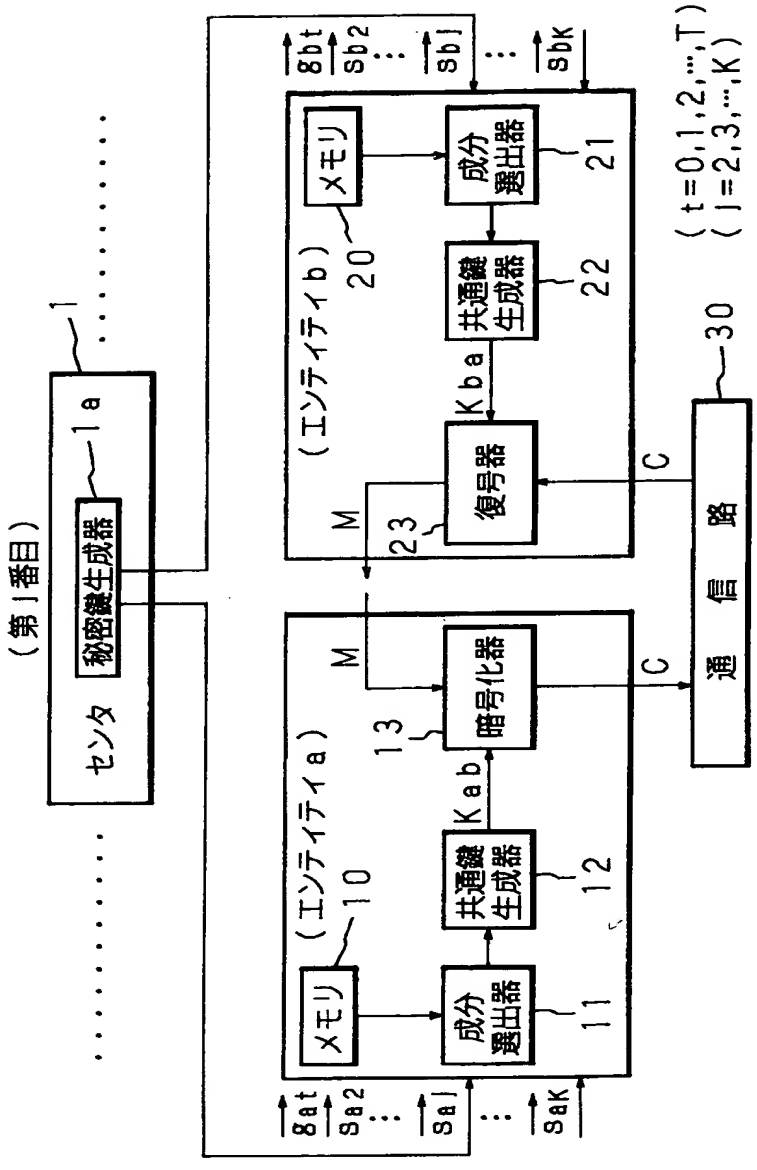
【図１】


1
1
センタ
（第1）
センタ
（第K）
$\vec{g}_{zt}$
$\vec{s}_{aK}$
$\vec{g}_{at}$
$\vec{g}_{bt}$
$\vec{s}_{bK}$
$\vec{s}_{zK}$
2b1
2a1
2aK
2bK
2z1
2zK
エンティティ
a
エンティティ
b
エンティティ
z
3ab
3bz
3az
(t=0,1,2,…,T)

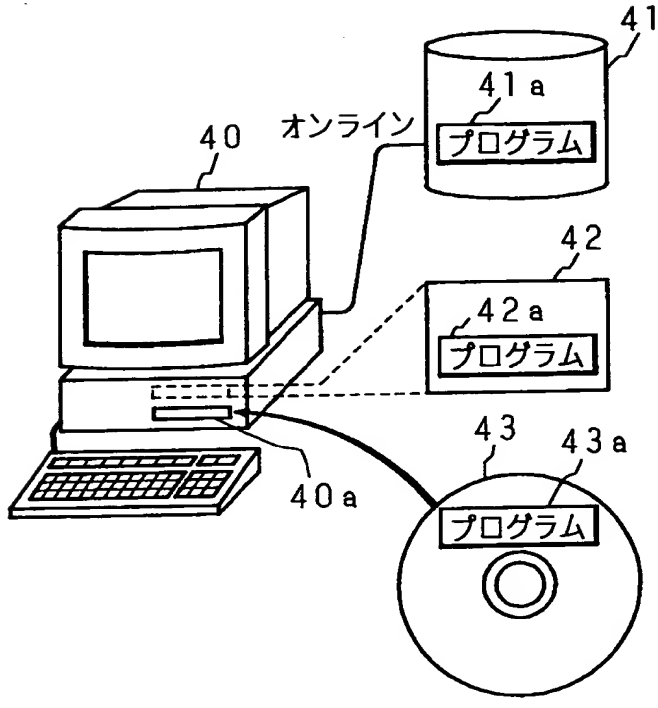
【図２】


IDベクトル（エンティティの特定情報）$\vec{I}_i$
$\vec{I}_{i1}$
$\vec{I}_{i2}$
$\vec{I}_{ij}$
$\vec{I}_{iK}$
M_1ビット
M_2ビット
M_jビット
M_kビット
Lビット

【図３】


（第ｉ番目）
センタ
秘密鍵生成器
1a
1
（エンティティａ）
10
メモリ
成分選出器
11
共通鍵生成器
12
Kab
暗号化器
13
M
C
（エンティティｂ）
20
メモリ
成分選出器
21
共通鍵生成器
22
Kba
復号器
23
M
C
通信路
30
sat sa2 sai saK
sbt sb2 sbi sbK
（t=0,1,2,…,T）
（i=2,3,…,K）

【図４】



【書類名】　　要約書

【要約】

【課題】　結託問題の回避を可能にし、その暗号系の構築が容易であるＩＤ－ＮＩＫＳによる暗号通信方法を提供する。

【解決手段】　各エンティティへ固有の秘密鍵を配布するセンタ１が複数設けられており、各エンティティの特定情報（ＩＤ情報）をいくつかに分割し、その分割した特定情報毎に作成したすべての秘密鍵をエンティティに配布する。各エンティティは、自身固有の秘密鍵に含まれている、相手のエンティティの分割特定情報に対応する成分を使用して共通鍵を生成する。

【選択図】　　図１

認定・付加情報

特許出願の番号	平成１１年　特許願　第０５９０４９号
受付番号	５９９００２０３１６０
書類名	特許願
担当官	塩崎　博子　　１６０６
作成日	平成１１年　３月１６日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】	000006297
【住所又は居所】	京都府京都市南区吉祥院南落合町３番地
【氏名又は名称】	村田機械株式会社

【特許出願人】

【識別番号】	598159964
【住所又は居所】	東京都渋谷区神宮前四丁目２番１９号
【氏名又は名称】	辻井　重男

【特許出願人】

【識別番号】	597008636
【住所又は居所】	大阪府箕面市粟生外院４丁目１５番３号
【氏名又は名称】	笠原　正雄

【代理人】　申請人

【識別番号】	100078868
【住所又は居所】	大阪府大阪市中央区釣鐘町二丁目４番３号　河野特許事務所
【氏名又は名称】	河野　登夫

次頁無

出 願 人 履 歴 情 報

識別番号　〔０００００６２９７〕

１．変更年月日　１９９０年　８月　７日
［変更理由］　新規登録
住　所　京都府京都市南区吉祥院南落合町３番地
氏　名　村田機械株式会社

出　願　人　履　歴　情　報

識別番号　　〔５９７００８６３６〕

１．変更年月日　　１９９７年　１月２１日
［変更理由］　新規登録
住　所　　大阪府箕面市粟生外院４丁目１５番３号
氏　名　　笠原　正雄

出　願　人　履　歴　情　報

識別番号　　〔５９８１５９９６４〕

１．変更年月日　　１９９８年１１月１９日
［変更理由］　新規登録
住　所　東京都渋谷区神宮前四丁目２番１９号
氏　名　辻井　重男